AO93 Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of
the premises located at 28736 North 20th Lane,
Phoenix, Arizona 85085.

Case No. 23-8488MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12/6/23 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11-22-23 10:00 am

Judge's signature

City and state: Phoenix, Arizona

Honorable John Z. Boyle, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is located at 28736 North 20th Lane, Phoenix, AZ 85085. It is located in the community named Fireside at Norterra. The real property is a two story unit and is the center townhome of a building comprised of three townhomes. The unit is constructed with mixed materials to include tan stucco and stacked stone in various brown hues.

The front door to the property faces east and is enclosed by a small courtyard with access via a black metal gate. The pillars on either side of the gate are a stacked stone connected to a stucco wall. The front door is located in a section of the build which is turret-like and stucco. The adjacent wall on the south side to the turret is stacked stone. Located on that wall the property address is displayed and reads "28736".

A driveway runs north and south on the west side of the property. Along this driveway, on the west side of the building are three two-car garage doors. The center garage door has the property address displayed and it reads "28736".

ATTACHMENT B

Property to be seized

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code Sections 1343 (Wire Fraud) and 1957 (Transactional Money Laundering) ("Subject Offenses"), described as follows, for the subject and his entities to include NOW MINING, VIP MINING, MILLENNIUM, BLOCK MINT, BLOCK X (BLK X), DIGITAL MINT, 888 MANAGEMENT, KANNABIZ KOIN (KK), KANNABIZ MONKEEZ, MY BLOCKCHAIN LIFE, WE SELL MINERS, JUSTICE CAPITAL, FX PRIMATY, and PHOENIX ULTRA, for the period May 1, 2017 through present:

1. Communications and other records concerning:

a. The formation, ownership, operation, control, corporate structure, registration, employees, contractors, customers, activities, and business/financial transactions of the subject or related entities;

b. The creation and mining of cryptocurrencies and their computer programming, identity of programmers, source code, and source and destination wallet addresses;

c. Purchases, sales, and other transactions involving cryptocurrency, cryptocurrency mining equipment, 3D printers, Raspberry Pis, graphics processing units (GPUs), graphics cards, computer and networking equipment (e.g., servers, routers, switches, cabling, WiFi devices, etc.), and solar panels and related equipment;

d. Investments in and purchases of investments, including communications with or about: (i) investors and potential investors; (ii) the development, marketing, or operation of the business, including promotional events, social media, and celebrity endorsements; and/or (iii) returns or anticipated returns on investment;

e. Multilevel marketing materials, including incentive structures and prizes, involving the subject or related entities;

f. Customer lists, logs, ledgers, journals, calendars, contracts, letters and memos, receipts, phone records, phone books, address books, and notations and other papers;

g. Customer orders, customer payments, and other documentation about sales of cryptocurrency, cryptocurrency mining machines, and hosting of cryptocurrency mining machines;

h. The registration of cryptocurrency exchanges and their regulation by the Securities and Exchange Commissions, Financial Crimes Enforcement Network (FinCEN), Department of Treasury, Arizona Corporation Commission, and other agencies;

i. Any real property or other assets owned, controlled, or occupied by SOWERBY and/or affiliates, including business associates, employees, family members, and affiliated trusts or businesses;

j. Any post office box or storage unit owned, leased, used, or possessed by SOWERBY and/or affiliates, including business associates employees, family members, and affiliated trusts or businesses; and

k. Any other records concerning the subject or his entities including individuals involved in the business; products or services provided by the business; advertisements and marketing of the business; emails and email servers; financial accounts; financial statements and ledgers; capital structure of the business; creditors and debtors; loans or credit; vendors and customers; assets of the business; any other property or equipment owned by or used by the business; investors; investments; the use of investment proceeds; and the acquisition of property, assets, or cash or cash equivalents obtained from such proceeds; and any records evidencing the attainment, secreting, transfer, concealment,

and/or expenditure of any such property, including receipts, invoices, other records of purchases, passwords, keys and other records tending to establish dominion and control of the property, including bank records, credit card records, wire transfer receipts, checks, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and receipts of money orders.

2. Records concerning financial transactions involving SOWERBY and/or affiliates, including business associates, employees, family members, and affiliated trusts or businesses;

3. Financial records belonging to SOWERBY and/or any business venture associated with SOWERBY, including bank statements, account opening documents, bank receipts, passbooks, bank checks, money market or similar account records, money drafts, letters of credit, money orders, cashier's checks, payroll documents, employer information, income and expense records, federal and state income tax returns or return information, loan applications, credit card records, records of any storage facility or safe deposit box, acquisitions, notes, bills, receipts, and other records reflecting anything of value including real or personal property, intellectual property, vehicles, aircraft or other vessels owned, purchased, sold or leased.

4. Any and all cryptocurrency, to include the following:

a. Any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;

b. Any and all representations of cryptocurrency private keys, whether in electronic or physical format;

c. Any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include "recovery seeds" or "root keys" which may be used to regenerate a wallet.

The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States.

5. United States currency in excess of $1,000, including the first $1,000 if more than $1,000 is seized.

6. Cash counting machines, money bands / currency straps, and any other devices or items indicative of the presence of large sums of cash.

7. Cryptocurrency mining machines, including pre-manufactured mining machines purchased from third parties and custom-made mining machines;

8. Computer equipment used to construct mining machines, including Raspberry Pis, 3D-printed cases, graphics processing units (GPUs), graphics cards, other equipment.

9. 3D printers.

10. Records concerning ownership and/or control of any real property, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, medication, personal telephone books, calendars, diaries, envelopes, registration, receipts, passwords, pictures or videos of clothing or other personal items, and keys that tend to show the identities of occupants, residents, owners, and users.

11. Evidence reflecting passwords, encryption keys, and other access devices that may be necessary to access relevant accounts or Subject Devices containing evidence of Subject Offenses.

12. Any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet

computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices (hereafter referred to collectively as "electronic storage media").

13. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

14. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:

a. all information related to the Subject Offenses, all bank records, checks, credit card bills, account information, or other financial records;

b. any information recording schedule or travel;

c. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;

d. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use, and events relating to crime under investigation and to the electronic storage media user;

e. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;

h. evidence of the times the electronic storage media were used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;

j. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;

k. records of or information about Internet Protocol addresses used by the electronic storage media;

l. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment;

n. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

o. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it.

15. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents,

programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

16. As used herein, the term "electronic storage media" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as moderns, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

17. Any records and information found within the digital contents of the electronic storage media seized showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

18. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact

information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

19. This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.